Employment Information Series

ELECTRONIC SURVEILLANCE:

A Discussion Paper

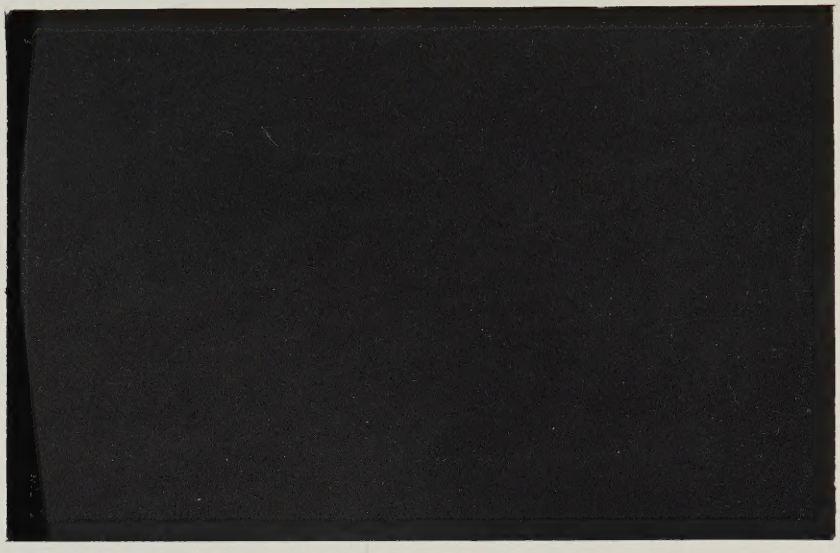
Number 21

Ontario

Ministry of Labour

Research Branch

Toronto
Ontario



ELECTRONIC SURVEILLANCE:

A Discussion Paper

Number 21

RESEARCH BRANCH

ONTARIO MINISTRY OF LABOUR

1979

Hon. Robert G. Elgie, M.D.
Minister

T. E. Armstrong, Q.C.
Deputy Minister

CONTENTS

SUMMARY

INTRODUCTION

As with other new technologies, the use of electronic surveillance devices offers benefits and exacts costs in ways which are far from clearly defined. Employers introducing such surveillance explain that they do so out of necessity to promote security, safety, and productivity.

The Issue

Employees, however, sometimes object that such surveillance is an invasion of privacy or causes psychological stress. At issue is how the conflicting interests of employers and employees can be resolved in particular circumstances. Although the paper focuses on electronic surveillance in the workplace, the broader issue of privacy both inside and outside the workplace cannot be ignored.

The Impetus

The conflict between privacy and surveillance is neither new nor unique to the workplace. Technological breakthroughs in surveillance technology, however, have produced a qualitative change in the nature of surveillance. It can now be total. The recent Puretex case has served notice that the time has arrived for a full public discussion of the general issue of electronic surveillance in the workplace.

CONCEPTS AND CONTEXTS

Definition

"Electronic surveillance" is the currently popular term for use of a growing variety of technological devices which allow the user to observe, hear, or otherwise become aware of actions, sounds and events related to the workplace. These devices may be classified as visual (e.g. closed circuit television, video replay), audio (e.g. wire tapping) or sensor (e.g. radar system).

Reasons for Use

The apparently most common motive for introducing electronic surveillance is to increase security, either at the perimeter of the workplace or inside it. Employee theft is considered by many employers to be reaching serious proportions.

Other reasons for introducing electronic surveillance are to protect the health and safety of workers, to control automated processes, and to improve employee productivity. Actual use of the devices may entail multiple motives.

Extent of Use in Ontario

Information on the extent to which electronic surveillance is used in Ontario is imprecise, although it is estimated that less than five per cent of firms with employees have introduced such equipment. This includes both work settings in which only employees are present and other locations such as shopping centres in which employees, clients and the general public may be observed. Visual surveillance, generally overt, is by far the most common type in Ontario.

Use of the devices is growing most rapidly in warehousing, retail stores, the clothing industry, jewellery manufacturing, financial institutions, high technology industries, monitoring of vending machines, and prisons and related institutions.

Alternatives to Electronic Surveillance

The alternatives to electronic surveillance cited by employers include increased supervision and personal searches of employees. The latter may be at least as unacceptable to employees as surveillance by electronic means.

Impact on Employees

Depending on the motivation for the devices and the manner in which they are introduced and applied, possible impacts on employees include increased psychological stress, loss of privacy, reduced sense of personal dignity, and strained relations with supervisors.

Employee Responses

The response of employees to electronic surveillance has varied greatly, depending on the circumstances. The most prevalent reaction in Ontario appears to be passive acceptance. This may be because use directly related to productivity improvement or employee theft may be infrequent. The data on specific use are unavailable. Such cases, where documented, appear to result in a negative employee response based on the argument that such surveillance is dehumanizing and not justifiable by the simple existence of an employment relationship.

PRIVACY

Meaning

One simple definition of privacy is "the right to be let alone." With respect to employee privacy, an extreme position taken by one American arbitrator was that an employee had absolutely no right of privacy during working hours in terms of the supervision of his work activities. This position has clear limits since it does not take into account the question of human dignity.

Need for Consent

The above-mentioned position appears to assume that consent to surveillance is automatic in the employment relationship. More commonly, however, it is argued that no consent exists if employees were not made aware of the surveillance as a term or condition of employment.

Balance of Values

Many arbitrators have recognized privacy as a human value in our society which has merit in the employment relationship. As such, it needs to be balanced against other rights and values (e.g. private property rights) and this balance may change over time depending on the extent to which each is endangered.

Quality of Working Life

One of the basic principles of Quality of Working Life relates to the specific issue of personal privacy in the workplace. It is argued that work policies and practices that treat workers as either replaceable parts of machines or as irresponsible will eventually cause harm to the workers, to the organization and its effectiveness and to society as a whole.

Other Possible Intrusions

In addition to electronic surveillance, other devices and practices in the workplace may conflict with individual privacy. These include such "lie detectors," as polygraphs and stress testers. At issue is whether an employer should be allowed to require a person to have his or her inner most knowledge and feelings probed as a condition of employment.

THE LEGAL CONTEXT

The Present State of the Law

In Ontario, the courts have not recognized and the Legislature has not created a legally protected interest in privacy. A right to privacy, however, has been judicially acknowledged in some other nations and, in three Western Provinces, it has received limited statutory sanction.

Common Law

The courts have been reluctant to protect privacy, partly because of the difficulty of proving or disproving the existence of emotional distress and translating it into damages, and partly because they have apparently not perceived it to be a sufficiently serious wrong. Currently, the only protection at common law against surveillance would be indirectly through some other cause of action, such as a campaign of harassment.

Arbitration

The only relevant jurisprudence arises out of arbitration of collective agreements under which the union alleges that the company has breached the contract by installing visual surveillance devices. Those cases, Canadian and American, generally have limited value since they interpret the particular terms of the individual contracts in the organized sector.

Recent Statutes Elsewhere in Canada

The British Columbia, Manitoba, and Saskatchewan Governments have enacted statutes pertaining to the right of privacy, although these would appear to have very limited applicability to the workplace. The Criminal Code of Canada prohibits, without authorization or consent, the listening to or monitoring of any oral communication.

The United States

A number of the American states have enacted privacy statutes similar to those in the western Canadian provinces. More significant, however, is the vigorous development of the common law. That development has established a doctrine of invasion of privacy outside the workplace, but it has little or no application to surveillance within the workplace.

ALTERNATIVE RESPONSES

Two non-legislative and a range of legislative models responding to the use of electronic surveillance are presented. Some major advantages and disadvantages are identified.

Common Law

1. Rely on the existing common law. This assumes that the continuing evolution of common law will eventually provide a solution through adaptation to changing social values and conditions.

Voluntary Standard

2. Depend upon voluntary compliance with guidelines developed through tripartite co-operation.

Legislative Remedies

3a. Recommend to the federal Minister of Justice that the present Criminal Code control of audio surveillance be extended to visual surveillance.

3b. Enact general privacy legislation similar to that of Manitoba, Saskatchewan, and British Columbia.

3c. Enact legislation creating a Privacy Ombudsman or Commission.

3d. Amend civil legislation to provide either for a pre-approval or licencing arrangement for electronic surveillance systems or for action on a complaint basis. Three existing Acts are mentioned.

i) The Employment Standards Act

ii) The Labour Relations Act

iii) The Human Rights Code

INTRODUCTION:
THE CURRENT ISSUE

ELECTRONIC SURVEILLANCE AND PRIVACY

Electronic surveillance is a subject of growing concern in technological societies. The use of such devices offers benefits and exacts costs in ways which are not yet clearly understood. The applications of such equipment have raised concerns about fundamental human values. On the one hand there is an employer's right to introduce electronic surveillance in the workplace and on the other, the right of privacy and the human dignity of employees in that workplace. At issue is how highly each right is valued and how the conflict of interests can be resolved in particular circumstances.

And The Larger Issue

This paper addresses the specific questions of the use and misuse of electronic surveillance in the workplace. Within the workplace itself, electronic surveillance is only one of a number of new technologies which may exacerbate intrusions upon personal privacy. While the workplace provides a focus for this discussion, privacy in a wider context cannot be ignored. The value attached to the employee's privacy in the workplace is inescapably influenced by the broader framework of the individual's right to privacy within society as a whole.

Employers Have Rights Too

Employers' use of electronic surveillance is often argued to be an exercise of a property right. Employers introducing such surveillance explain that they do so to promote security, safety and productivity. To regulate or prohibit electronic surveillance would presumably abridge their rights and damage their business. If an employee feels that his or her privacy has been unacceptably abridged, it may be argued that the employee is always free to terminate the employment relationship.

The Dilemma Is Not New

The conflict between privacy and surveillance is not new. Supervision has traditionally entailed surveillance of employees' activities in the workplace in much the same way as teachers watch students, parents watch their children, and policemen watch the citizenry. In each example, there has been perennial debate over how much surveillance is appropriate and at what point it becomes harassment.

New Technology Forces The Issue

Breakthroughs in technology have produced a qualitative change in the nature of surveillance. Electronic surveillance can now be total and constant. Such pervasive surveillance invokes images of Huxley's Brave New World and Orwell's 1984. Previously, surveillance in the workplace was limited by the availability of supervisory resources. Also, while human surveillance usually allowed employees to be aware that they were being watched or overheard, electronic technology makes covert surveillance much easier.

Impetus of The Puretex Case

Electronic surveillance is far more widespread, and the consequent debate over privacy more fiercely joined, in other jurisdictions such as the United States. In the autumn of 1978, however, public attention in Ontario was drawn to a strike at the Puretex Knitting Company Limited in North York. One of the items of disagreement between the Company and its workers, represented by the Canadian Textile and Chemical Union, was the installation of closed circuit television monitoring equipment. While the two parties eventually reached agreement to remove one camera, and submit to arbitration[1] the future use of other cameras, this case stimulated public interest. The general issue of electronic surveillance in the workplace has been debated in the Legislative Assembly and two private members bills have been presented. The time is appropriate for a full public discussion of the general issue of electronic surveillance in the workplace and this paper is intended to foster that discussion.

---

1. Puretex Knitting Company Limited and Canadian Textile and Chemical Union. Unreported decision of Mr. S. R. Ellis, arbitrator, dated May 29, 1979.

CHAPTER ONE:
ELECTRONIC SURVEILLANCE - CONCEPTS AND CONTEXTS

This section defines electronic surveillance, reviews reasons for its use in the workplace, examines the extent and nature of electronic surveillance in Ontario and provides an overview of employee reaction to such surveillance.

WHAT IS ELECTRONIC SURVEILLANCE?

"Electronic surveillance" in the workplace is the currently popular term for the use of a variety of technological devices which allow the user to observe, hear, or otherwise become aware of activity inside the workplace proper (internal surveillance) or in related areas such as loading docks and parking lots (perimeter surveillance). This definition is necessarily broad: its breadth derives from continuing technological advances originally developed by the military and subsequently adapted for civilian uses. For practical purposes, the devices may be classified as visual, audio, and sensor.

Visual

Literature on the topic, mainly American, suggests that visual surveillance devices are those most commonly being introduced within the workplace. They vary from still and motion cameras through visual "screens" that appear to be opaque walls, and "scanners" to read the contents of unopened envelopes.[2] The last of these, with various other unusual devices which will not be described here, are more likely to find use in industrial espionage than in employee surveillance.

Still or motion camera systems have generated the most employee opposition. The closed circuit television (CCTV) system allows continuous or near-continuous observation of multiple locations from a single console. A permanent record can be provided on tape and observers can "zoom" in on an individual or object for close observation. Many ordinary CCTV systems allow for accurate photographs in near-total darkness and an infrared capability can readily be added. Dummy cameras can be included to give the impression of surveillance when it is not occurring, and optic fibre technology allows the user to "see around corners". Compact mobile cameras can fit into a vest pocket.

Audio

Audio surveillance devices vary from a "listening" capability built into an ordinary intercom or public address system through logging or monitoring the content of telephone conversations and installing the classic "bug" microphone and transmitter. Directional microphones can be focused on conversations being

---

2. A. F. Westin, Privacy and Freedom (New York: Atheneum, 1968), ch. 4.

conducted at a considerable distance, and tape recorders can provide permanent records of conversations. The combination of computer and "voice print" offers a future capability of tape scanning of all recorded conversations to print out only those of particular individuals or those containing selected "key" words.[3]

Sensor

Sensor surveillance devices may be introduced where visual or audio types are considered inadequate. The most common are light sensors, such as the familiar "electric eye" on automatic doors, but the sensory types include radar systems and signal transmitter "tags" which allow the system user to trace electronically the movement of people and products. One Canadian arbitration case[4] is notable for dealing with a form of sensory device called a "tachograph" which automatically recorded time and rate of engine speeds of trucks and therefore also of the truck drivers.

REASONS FOR ELECTRONIC SURVEILLANCE

Employers introduce electronic surveillance equipment for various reasons, but essentially as an extension of limited human capabilities. Whether the purpose of the surveillance is security (e.g., to deter theft), health and safety (e.g., to monitor safety control), controlling automated processes (e.g., on production lines), training (e.g., of new workers) or employee productivity (e.g., time and motion study), such monitoring is usually an attempt to increase the duration and dependability of supervision. Some of these objectives could, in at least some instances, be met equally well by recruiting additional supervisory personnel, generally at a considerably greater cost.

Security

Firms purchasing electronic surveillance systems give security as their primary motive, to protect private property against theft, vandalism and sabotage by employees or others, and also to counter industrial espionage. Surveillance for security reasons can be directed at either or both the perimeter or interior of the premises depending on the perceived threat.

Theft by employees is often cited as a serious concern for industry. Figures from the United States are frequently quoted to demonstrate the severity of this problem. According to one estimate, by 1977 American business was losing between $12 billion and $40 billion annually to internal employee crime.[5] The United States Department of Justice has estimated that office

---

3. Ibid., ch. 4.

4. Re Milk and Bread Drivers, Local 647 and Dominion Dairies Ltd. (1969), 20 L.A.C. 315.

5. C. Craver, "The Inquisitorial Process in Private Employment", in Cornell Law Review, vol. 63, (1977), pp. 1-64.

crime is doubling every three years, and one insurance company asserts that the theft of office equipment was one of its five leading corporate loss items.[6] Based on a recent survey of selected Ontario industries, it is estimated that one in seven Ontario firms experience serious problems with employee theft and sabotage.[7] Furthermore, it appears that employers are increasingly convinced that electronic surveillance systems are the most effective and least expensive solution to the growing problem of material losses. Many employers hold this conviction in regard to a deterrent value, even though they do not know the extent to which losses are reduced through surveillance.

Health and Safety

Surveillance by electronic means is also introduced to protect the health and safety of employees. A camera or other surveillance device may be focused on a work process difficult or dangerous for direct human observation - for example, in locations where radiation, high temperatures, or toxic dusts are present. The employees themselves may be responsible for monitoring. In some instances, however, work areas are monitored to ensure that jobs are being carried out in a manner consistent with company rules and applicable health and safety legislation. Increased on-the-job use of alcohol and drugs has been identified as undermining occupational safety as well as production efficiency. In 1975, one in six Ontario companies reported that they were experiencing serious problems with alcoholism.[8]

Controlling Automated Processes

Automated work processes may be monitored in order to maintain efficient production and quality control. The equipment is usually focused on the specific process or machine and not on a general work area. Again, the electronic surveillance may be carried out by employees rather than supervisory personnel.

Employee Productivity

Monitoring for purposes of ensuring that employees are productive or for improving productivity is perhaps the most contentious use. Employers may survey not only production areas, such as assembly lines, but also internal non-production areas, such as lunchrooms and washrooms. Specific applications may include time and motion studies, monitoring conversations to see if they are work related or "time wasting", observing washroom visits, etc.

---

6. P. Kramarsky, "Surveillance Systems: Managements Electronic Sentries" in Administrative Management, vol. 27, (1966), pp. 41-50.

7. G. Robertson, "Absenteeism and Labour Turnover in Selected Ontario Industries", in Relations Industrielles, vol. 34, number 1, (1979), p. 93.

8. Ibid.

Multiple Reasons

Electronic surveillance may be used for more than one reason. Even when the primary purpose of electronic equipment in a work area is security, as an example, employees are never certain that the equipment is not also monitoring their productivity.

EXTENT OF ELECTRONIC SURVEILLANCE IN ONTARIO

In an effort to determine the extent to which electronic surveillance is used in Ontario workplaces, distributors of electronic surveillance equipment, security firms, individuals in the labour movement, and companies using electronic surveillance devices were contacted. It was not possible to compile precise information, although impressions can be formed. It is estimated that several thousand organizations in Ontario (representing less than 5% of firms having employees) are now using some form of electronic surveillance. Present applications include installations in both work-related locations and in more general public areas, such as shopping centres. Further, the use of electronic surveillance is growing rapidly, although it is not known what proportion of installations are in locations which employees find objectionable.

Video Surveillance Most Common

While applications exist in Ontario work settings of video, audio and sensor surveillance, visual equipment - including closed circuit television (CCTV) and video tape recorders (VTR) - is by far the most common. Where the purpose of surveillance is to monitor either work flow or highly automated work processes, the cameras are focused on the machines and not the employees per se. Where the monitoring is intended either as a means of controlling theft or to ensure safe work practices, the employees themselves are often the object of surveillance. Sources indicate that general or unlimited surveillance of the workplace appears to be rare in Ontario. However, it is understood that in those industries where electronic surveillance is most prevalent, the devices are normally concentrated in or limited to specific areas where expensive or sensitive items are located, or to loading docks, etc.

Usually Overt Surveillance

The video equipment located in the working environment in Ontario is normally overt. Hidden cameras are used, but this is generally to deal with a special problem (e.g., theft of petty cash) in a specific location. Covert surveillance devices tend to be removed once the problem is solved.

Where Surveillance is Growing

Information provided by equipment distributors suggests that electronic surveillance is growing most quickly in:

- warehousing, including shipping and receiving areas. The concern here is generally theft and vandalism; however, in some situations electronic surveillance is used to monitor for accidents.
- retailing of all types to control both employee theft and shoplifting by customers.
- the clothing manufacturing industry. Employers report that video equipment is used to discourage employee theft, to ensure quality control and employee safety, and to prevent industrial espionage. One Ontario company reported that employee theft fell from about $1000 per week to less than $25 per week after the installation of a CCTV.
- jewellery manufacturers and other establishments using precious metals, to control employee theft.
- banks and related financial institutions to discourage robbery.
- high technology industries of all types (e.g., electronics industry). In these situations video surveillance is used to ensure quality control, discourage employee theft and prevent industrial espionage.
- in areas where vending machines are located, to discourage vandalism and theft.
- in special institutions (e.g., detention centers, psychiatric wards). In these situations audio and visual surveillance is used to ensure employee safety.

ALTERNATIVES TO ELECTRONIC SURVEILLANCE

A number of employers indicated that, if electronic surveillance were prohibited, they would give serious consideration to increasing the numbers of supervisory personnel and/or subjecting employees to a search as they left the premises, at least on a spot check basis.

Personal Searches

This raises the question of whether searches of personal effects are more demeaning than the use of electronic surveillance, and whether the prohibition of electronic surveillance would lead to an increase in the use of personal searches as a means of controlling theft.

POSSIBLE IMPACT ON EMPLOYEES

The possible impact of surveillance on employees includes increased psychological stress, loss of privacy and diminished sense of personal dignity, strained relations with supervisors, etc. The judgement of Ellis in Puretex refers to these three possible results, and identifies several contributing factors such as whether the surveillance is continuous, permanent, covert or overt, and the lack of possible assurance that it is being used solely in the individual employee's best interest.

THE EMPLOYEE RESPONSE

According to the American literature, employee response to the installation of electronic surveillance systems varies according to the nature of the workforce; the type and extent of system installed; the firm's health, safety, and security experience; whether the employees are organized and bargain collectively; whether the employees were consulted prior to installation of the system; whether the system is covert or overt and, if covert, how its use was discovered; and, generally, according to the quality of working life within the firm. Employees appear to have received the introduction of some systems, particularly of limited surveillance, with trust or passive acceptance. Given the increasing deployment of such systems in Ontario and the small number of complaints made to Government or known to central union organizations or civil liberty groups, it would appear that most employees accept surveillance as a necessary part of their working environments. In some situations, however, particularly in the United States, where large, intrusive systems are more common, employees have responded with unease and even outrage.

... To Security Reasons

Employee response to perimeter security systems has frequently been to support applications such as video-surveillance of parking lots where theft or vandalism of company and employee vehicles has occurred.

The literature also indicates that employees have had a greater tendency to object to the installation of electronic surveillance systems for internal security purposes, on the grounds that they are inappropriate and offensive. Employees and their representatives have argued that electronic surveillance may confer on the employer the benefit of increased internal security but it exacts a price from all employees in terms of privacy and human dignity. It is argued that internal

security problems should be solved by other means. However, as Ellis has observed in the Puretex case, if employees could be pursuaded that surveillance was directed exclusively at deterring theft, and not at monitoring their performance, it may not be a source of stress.

... To Productivity Reasons

The response of employees to electronic surveillance systems used for studying and increasing productivity is similar to but stronger than their response to internal security systems. When surveillance is directed at productivity, employees have complained of its dehumanizing effect in reducing the employee to the status of the inhuman cog in a machine. This reaction has perhaps been most vividly portrayed in Chaplin's Modern Times.

... Through Collective Bargaining

The various employee responses to electronic surveillance are articulated through existing channels for the expression of employee concerns. In firms whose employees are unionized, this may mean grievances, the negotiation of protective provisions through collective bargaining, and even strike action. While utilizing these, however, employees and their representatives have responded that the burden of action is inappropriately placed. If a right to privacy exists, they argue, then it should be a basic human right protected by legislation. As well, this would extend protection to the majority of the workforce which is not unionized.

CHAPTER TWO:
THE MEANING OF EMPLOYEE PRIVACY

The first part of this chapter reviews a number of definitions of the general concept of personal privacy, then addresses the meaning of privacy within the employment relationship and identifies a number of other areas of concern related to employee privacy.

WHAT IS PRIVACY?

A concise definition of personal privacy was provided by Justice Cooley in 1888: "the right to be let alone".[9] A more recent definition was proposed by Mr. Brian Walden in a Bill introduced in the British Parliament in 1969:

> (1) 'Right of privacy' means the right of any person to be protected from intrusion upon himself, his home, his family, his relationships and communications with others, his property and his business affairs, including intrusion by:
>
> (a) spying, prying, watching or besetting;
>
> (b) the unauthorized overhearing or recording of spoken words;
>
> (c) the unauthorized making of visual images;
>
> (d) the unauthorized reading or copying of documents;
>
> (e) the unauthorized use or disclosure of confidential information, or of facts (including his name, identity or likeness) calculated to cause him distress, annoyance or embarrassment, or to place him in a false light;
>
> (f) the unauthorized appropriation of his name, identity or likeness for another's gain.[10]

In Ontario, Professor E. F. Ryan, in a 1968 study for the Ontario Law Reform Commission, chose to begin his "Protection of Privacy in Ontario, A Preliminary Study", by quoting the conclusions of the Nordic Conference on The Right to Privacy that:

> The right to privacy is the right to be let alone to live one's own life with the minimum degree of interference. In expanded form, this means:

---

9. Quoted in Report of the Committee on Privacy, The Rt. Hon. Kenneth Younger, Chairman, (London: Her Majesty's Stationery Office), July, 1972, Appendix K, pp. 327-328.

10. Ibid.

> The right of the individual to lead his own life protected against: (a) interference with his private, family and home life; (b) interference with his physical or mental integrity or his moral and intellectual freedom; (c) attacks on his honour and reputation; (d) being placed in a false light; (e) the disclosure of irrelevant embarrassing facts relating to his private life; (f) the use of his name, identity or likeness; (g) spying, prying, watching and besetting; (h) interference with his correspondence; (i) misuse of his private communications, written or oral; (j) disclosure of information given or received by him in circumstances of professional confidence.[11]

Professor Ryan immediately pointed out, however, that even this listing did not cover data banks and confidential matters relating to group or corporate existence rather than to individual privacy. He concluded that "More elaborate definitions are possible, but would not necessarily be of any more practical value."[12]

WHAT IS EMPLOYEE PRIVACY?

Employee privacy is no less difficult to define. Simply, it is individual or group (employee organization) privacy as conceived within the employment relationship. This paper will not attempt to discuss the entire range of privacy conerns within the employment relationship, but will focus instead on that aspect of employee privacy which relates to surveillance. The scope of the paper does not include the broad range of privacy issues, such as those being investigated by the Commission on Freedom of Information and Individual Privacy (Dr. D. C. Williams, Chairman) and The Royal Commission of Inquiry Into The Confidentiality of Health Records in Ontario (Hon. H. Krever, Commissioner). Unless otherwise stated, therefore, the phrase "employee privacy" will henceforth in this paper be used in the focused sense. The key concepts of employee privacy are those of consent, the overt or covert nature of actions, and dignity.

---

11. H. Allan Leal, Q.C., Chairman, Report on the Protection of Privacy in Ontario, (Department of the Attorney General, 1968), Appendix, p. 7.

12. Ibid.

At the extreme is the view that an employee has no right of privacy during the working hours as far as the supervision of his work activities are concerned. This has been held by the American arbitrator, Richard Mittenthal, in the case of FMC Corp. v. U.A.W. [13]

> The right of privacy concerns an individual's right not to have his statements, actions, etc., made public without his consent. But this serves only to protect him against the publication of his PRIVATE statements or PRIVATE actions. It should be evident that an employee's actions during working hours are NOT PRIVATE actions.

CONSENT AND DIGNITY

The position taken by Mittenthal appears to be that consent is automatic with the establishment of an employment relationship, unless otherwise specified in an employment contract, government legislation, or elsewhere. However, others could argue that such a position has inherent limitations and that employees do not, in fact, automatically extend consent to electronic surveillance and all other employer actions which may reduce privacy. An example which illustrates the inherent limits is any situation in which social values are strong. An example of this might be surveillance of a washroom, particularly surveillance monitored by someone of the opposite sex. In this situation, objections would be raised in terms of the more basic concept of human dignity.

OVERT OR COVERT SURVEILLANCE

The idea of consent is also related to whether surveillance is covert or overt. If employees are subjected to electronic surveillance without being informed that they will be under scrutiny, then clearly they are denied the opportunity to consent or protest.

A BALANCE OF VALUES

Many arbitration awards comment upon or apply what is essentially a balance of values in determining the impact of surveillance on privacy. Without necessarily determining the nature of an employee's right to privacy or, even whether such a right exists, arbitrators have generally recognized privacy as a human value which has meaning in the employment relationship. As such, it must be balanced against other rights and values (e.g., private property rights). That balance is not absolute, but changes over time, based on the extent to which each value or

---

13. 46, Lab. Arb. 335 [1966] or 66-1 CCH Lab. Arb. Awards, para. 8287 [1966].

right is endangered. Applying this balance of values in a case where theft was documented as being a serious problem for a firm, arbitrator Mr. Guy Dulude in Liberty Smelting Works (1962) Ltd., and the U.A.W., Local 1470 (1972)[14] held that cameras could be installed but the following conditions were imposed on their use:

a) the company would not under any pretext set its cameras upon any particular employee in a constant manner;

b) the use of the cameras was to be limited to three and the number of monitors to two;

c) the use of the cameras was to be strictly limited to the prevention of theft, and

d) if at any time the extraordinary need of theft prevention were to disappear, the decision could be revised and the company would bear the burden of proving the necessity for maintaining the system.

A similar application of balance of values can be found in the recent case of Puretex Knitting Company Ltd. and the Canadian Textile and Chemical Union (1979). In this case the arbitrator, Mr. S. R. Ellis, found that the use of cameras in the production area of the plant could not be justified because the stated reason for the introduction of the cameras, theft and pilfering, was not found to be a problem of serious proportions. On the other hand, Mr. Ellis ruled that the cameras in the storage areas, the loading dock area, and the parking lot area could remain.

QUALITY OF WORKING LIFE

Concern about personal privacy in the workplace is directly related to one of the basic principles of the concept of quality of working life (QWL): that the individual worker is a whole human being and should be treated as such.

Policies and practices which treat workers as either replaceable parts, or as irresponsible, will eventually do serious harm not only to the workers themselves, but also to the organization and its effectiveness, and to society as a whole.[15]

---

14. 3 S.A.G. Vol. III, No. 8, 1035.

15. See, for example, J. R. Hackman and J. L. Suttle, Improving Life at Work: Behavioural Science Approaches to Organizational Change. (Santa Monica, California: Goodyear, 1977). See also R. Tannenbaum and W. H. Schmidt, "How to Choose a Leadership Pattern," in Harvard Business Review, vol. 36 (March-April, 1958), pp. 95-101.

Proponents of Quality of Working Life agree that since the values, needs and intelligence of people do not change when they enter the workplace, there is no reason why the rights and responsibilities they enjoy as citizens should be withheld from them in their role as workers. Initial experiences of the Ontario Quality of Working Life Centre, as well as An Inventory of Innovative Work Arrangements in Ontario, indicate that these values are gaining recognition in Ontario.[16]

OTHER POSSIBLE INTRUSIONS

The emphasis in this paper is on electronic surveillance and the extent to which it may infringe on employee privacy. In order to understand fully the scope of the problem it is important to examine various other devices and practices that may limit individual privacy in the workplace.

Polygraphs and Other "Lie Detectors"

The polygraph is the most established and widely known of a group of devices generally referred to as "lie detectors". The theory behind the operation of a polygraph is that unique physiological signals are given when a person is under stress, and that persons are under stress when they are not telling the truth. Even though a number of jurisdictions have severely limited their use because of concerns regarding unreliability, technological development continues.

In recent years instruments called psychological stress evaluators (PSE) and psychogalvanic meters (PGM) have been introduced as "lie detectors" measuring the stress in a voice and changes in the electricity of the skin respectively.[18] A recent magazine article reports that a PSE will be on the market by the end of the year, built into a wristwatch, at a cost of under thirty dollars.[19]

The debate on the use of polygraphs, similar to that on electronic surveillance, raises questions of whether the use is overt or covert and whether the employee has consented to a "lie detector" test specifically or whether the contractual employment arrangement implies consent. If an employee refuses to submit to such a test to "prove" himself not guilty of theft, employers may reason that this implies a probability of guilt. An applicant for employment who refuses a test may be denied employment as a result.

---

16. Research Branch, Ontario Ministry of Labour, Jacquie Mansell, ed., An Inventory of Innovative Work Arrangements in Ontario, 1978.

17. See, for example, D. J. Purich, "The Truth About Lie Detectors", in Canadian Lawyer, vol. 3, No. 2 (June, 1979), pp. 29-30.

18. Dan Dorfman, "The End of Trust?", in Esquire, vol. 91, No. 8 (April 24, 1979), pp. 8-9.

CHAPTER THREE:
THE LEGAL CONTEXT

The Chapter contains a description of the current legal context, both of privacy generally and of its specific application to the workplace.

THE PRESENT STATE OF THE LAW RESPECTING SURVEILLANCE

In Ontario, most other Provinces, and Great Britain, the courts have not recognized and the legislatures have not created legally protected interests in privacy. A right to privacy, however, has been judicially acknowledged in some otherjurisdictions, and it has received limited statutory sanction in three western provinces. The protection of privacy through civil and criminal measures has been advocated in Ontario[19].

THE COMMON LAW POSITION

The common law protects a person's property, emotional and psychological well-being (to a limited degree), physical well-being, and reputation. These various protections can be found in the actions for the civil wrongs (or "torts") of trespass, battery, intentional causing of emotional distress, and defamation. However, no case has yet arisen in which such values as privacy or personal dignity have been protected, although the courts may at some future time bring these values within the protection of the law. In fact, the issue has expressly been left open by one court in Ontario.[20]

There appear to be two prevalent attitudes which account for the action of the courts on privacy: a subjective one that emotional distress is not a serious concern but an everyday phenomenon to which all individuals are subject; and a practical one that emotional distress is too vague a concept for the courts.

---

19. See e.g., Ontario Law Reform Commission, Report on the Protection of Privacy, 1968.

20. See Krause v. Chrysler Canada Ltd. (1970), 12 D.L.R. (3d) 463 (Ont. H.C.), 1972, 25 D.L.R. (3d) 49 (Ont. H.C.), rev'd, on unrelated grounds, (1974), 1 O.R. (2d) 225 (C.A.).

The first attitude is illustrated by Flamm v. Van Nierop[21], an action against the defendant for intentionally causing emotional distress to the plaintiff by constantly harassing him in public by making faces at him, rushing up to him, following him too closely in his car, and telephoning him and then hanging up. In his judgement, J. Dillon described the kinds of interests that the law of torts protects:

> The law cannot be expected to provide a civil remedy for every personal conflict in this crowded world. Physical injuries to the person, inflicted either intentionally or through negligence, are actionable under familiar principles. Acts causing mental distress are in a different category. Oral or written statements which are false and defamatory, and which upon publication tend to deprive the victim of his good name, may be remedied in actions for libel and slander... On the other hand, offenses of a minor nature, such as name-calling or angry looks, are not actionable though they may wound the feelings of the victim and cause some degree of emotional upset. This is because the law has no cure for trifles. But when the actor's conduct is extraordinarily vindictive it may be regarded as so extreme and so outrageous as to give rise to a cause of action for emotional distress.

The second attitude is expressed by J. Fleming Jr. in The Law of Torts[22]:

> The right of privacy has not so far, at least under that name, received explicit recognition by British courts... some of this hesitation is undoubtedly due to the fact that we are here concerned primarily with injury in the shape of mental distress, which has so frequently evoked the fear of opening the door to fanciful claims. Another factor is the difficulty of drawing a clear line between what should and should not be permitted. The mere fact of living in the complex society of today exposes everyone to annoying contacts with others, most of which he must bear as the price of social existence.

---

21. (1968) 291 N.Y.S. 2d 189 (N.Y.S.C.)

22. 5th Ed., (Boston: Little, Brown, 1977), pp. 590-1.

Common Law and Surveillance

The practical consequence is that no cause of action exists at common law to compensate a plaintiff for the emotional distress and affront to dignity caused by surveillance. In Re Copeland and Adamson[23], it was held that there was no protection at common law against surveillance of oral conversations (here: wiretaps of telephone conversations, prior to the enactment of the Criminal Code provisions authorizing certain wiretaps). And in cases such as Victoria Park Racing Co. v. Taylor[24], it was held that there is no protection at common law against visual surveillance of one's actions. (Also, see Frey v. Fedoruk[25] where it was held that being a "peeping Tom" was not an offence at common law).

Since no cause of action exists to compensate a plaintiff for surveillance in and of itself, the defendant would have to do something more to give rise to a claim for damages. For example, if the surveillance were carried out as part of an unjustified campaign of harassment deliberately intended to cause the victim emotional suffering, or negligently causing emotional suffering, then there would be a cause of action for intentionally causing emotional distress or for negligence; if the surveillance were carried out against a person's property in order to intimidate the victim into doing certain things, a cause of action for watching and besetting could be maintained. None of these types of conduct, which involve surveillance, applies to the question of surveillance in the workplace because the employer is conducting the surveillance on his own property, his intention is not to cause emotional distress, and negligence could rarely be proven.

Arbitration Cases

Since the law recognizes and enforces rights arising under contracts, an enforceable right is created where a person who is conducting the surveillance agrees to desist. It is for this reason that the jurisprudence dealing with the issue arises in arbitration cases concerned with the interpretation of collective agreements. In these arbitrations, the union alleges that the company has breached the contract by installing visual surveillance equipment. These cases, both Canadian and American, do not state any legal principles of general application; rather they are simply based upon rights under collective agreements.

---

23. (1972), 28 D.L.R. (3d) 26

24. (1937), 58 C.L.R. 479

25. (1950), S.C.R. 517

Many of these cases are referred to in the Puretex arbitration decision. The conclusion that is consistently reached in all the cases is that the company has the right to install surveillance equipment if the particular contract contains a broad "management rights" clause by which the company retains authority over all matters of supervision of employees which have not been expressly bargained over and referred to in the contract. Where there is no "management rights" clause, but a clause forbidding management from altering any condition of employment that is "beneficial" to the employees and that has not been expressly referred to in the contract, the cases hold that no surveillance system may be installed. This conclusion is based on the premise that it is not "beneficial" to the employees to be under constant electronic surveillance.

These decisions, based upon principles of contract law, are of no direct assistance to those employees who are not governed by a collective agreement. In such cases, the employer has the legal right to initiate visual and other non-auditory electronic surveillance.

RECENT STATUTES

The Federal jurisdiction and the provinces of British Columbia, Manitoba and Saskatchewan have, in the last several years, enacted statutes pertaining to the right to privacy.[26] While none of these statutes specifically addresses the issue of electronic surveillance in the workplace, they bear some relevance to this problem and, more generally, reflect a growing concern for the integrity of private conduct and communications.

Federal

The Protection of Privacy Act[27], amended the Criminal Code so as, inter alia, to create offences relating to the interception of private communications, the disclosure of private communications, and the possession of any device primarily useful for the surreptitious interception of such communications. "Intercept" is defined so as to include listen to, record or acquire a communication, or its substance, meaning or purport. "Private communications" refers to oral or tele-communications made under circumstances in which the originators may reasonably expect that they will not be intercepted by anyone other than the intended recipient. The wilful interception of a private communication "by means of an electromagnetic, acoustic, mechanical or other device" is an indictable offence subject to five years imprisonment. However, judicially authorized or consented-to interceptions are exempted from this penal provision.

---

26. Privacy legislation, Bill 70, was also introduced into the Nova Scotia Legislature in 1972, but it did not go beyond First Reading.

27. S.C. 1973-74, c. 50.

The effect of these Criminal Code amendments is to render criminally liable anyone in Canada who, without authorization, intentionally listens in on, or monitors, oral communication without the express or implied consent of one or more of the parties. While this legislation thus has some obvious relevance to the use of audio "bugs", it has no bearing on the more common employee-monitoring devices, such as closed-circuit television (CCTV), which utilize visual rather than aural forms of surveillance.

British Columbia

The Privacy Act[28], was the first legislation of its kind in the Commonwealth. Among other things, the Act creates a tort, or civil wrong, actionable without proof of damage, for the violation of privacy, wilfully and without claim of right. Privacy is not defined, but its violation may occur by "eavesdropping or surveillance, whether or not accompanied by trespass", and the court's attention is directed to certain factors in deciding the issue:

> s.2(2): The nature and degree of privacy to which a person is entitled in any situation or in relation to any matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of another, regard shall be given to the nature, incidence and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties.

Several significant exceptions are described in the statute. Among the activities which do not constitute invasions of privacy are those consented to by a person entitled to consent, an act authorized or required by law, the acts of police or public officers engaged in the investigation of criminal or provincial offences, and, most directly germane to the issue of privacy in the workplace, conduct incidental to the exercise of a lawful right of defence of person or property.

Although hailed as a significant development at the time, only one decision dealing with the Act has since been reported: Davis v. McArthur.[29] In Davis, a private detective was successfully sued, at trial, for his use of electronic surveillance equipment during a divorce investigation. On appeal, however, the detective was absolved of liability, the court being

---

28. S.B.C. 1968, c. 39.

29. (1970), 10 D.L.R. (3rd) 250 (B.C.S.C.), rev'd (1971, 17 D.L.R. (3rd) 60 (C.A.).

of the view that he had acted reasonably "in the circumstances" as per s.2(2). In light of this decision and the statutory exceptions, the B.C. Privacy Act is likely to be of little assistance in efforts to control electronic surveillance in the workplace.

Saskatchewan

Under the Privacy Act[30], the statutory tort of invasion of privacy is virtually identical to that enacted in British Columbia; i.e., the wilful violation of the privacy of another, without claim of right, having regard to what is reasonable in the circumstances and the lawful interests of others. The Saskatchewan legislation, like that of Manitoba (see below), grants the Court a broad discretion as to remedies, including damages, injunction, and other relief which appears necessary under the circumstances. The British Columbia statute has no comparable provision. The statutory defences available to a defendant are essentially the same as those delineated in the British Columbia legislation. One unique aspect of the Saskatchewan Act is that proof of any of the statutory illustrations of invasion of privacy, including "surveillance, auditory or visual ..., of a person, by any means", without consent is prima facie evidence of a violation of privacy.

However, a defendant may still vindicate himself by showing that such conduct was "incidental to the exercise of a lawful right of defence of person or property." To date, there have been no reported cases involving the Saskatchewan statute.

Manitoba

The Privacy Act[31] creates a somewhat different tort than that enacted in British Columbia and Saskatchewan. In Manitoba, a person commits the wrong when he substantially, unreasonably, and without claim of right, violates the privacy of another by, among other means, auditory or visual surveillance. Thus, unlike the case in British Columbia and Saskatchewan, there exists the possibility of an action for negligent, as well as intentional, invasion of privacy. However, the Manitoba statutes make it a defence for the defendant to show that he neither knew nor should reasonably have known that his acts would have violated the privacy of any person. The additional defences described in the British Columbia and Saskatchewan statutes are essentially duplicated in the Manitoba legislation. And again, the action may be brought without proof of damage. The protection conferred by the Manitoba statute also differs from that available in British Columbia and Saskatchewan in that the court's regard to "the circumstances of the case" (including such matters as the nature, incidence

---

30. S.S. 1974, c. 80.

31. S.M. 1970, c. 74.

and occasion of the offending conduct, the effect of the violation, and the relationship between the parties) relates solely to its assessment of damages and not its determination of the substantive issue. An additonal unique feature of the Manitoba statute is a provision declaring that evidence obtained by virtue or in consequence of a violation of privacy in respect of which an action may be brought under the Act is inadmissable in any civil proceedings. This exclusionary rule of evidence would, it appears, apply to labour arbitration hearings.

To date, there have been no reported cases under the Manitoba legislation.

LIMITS OF PROVINCIAL LEGISLATION

One common feature of the three provincial privacy statutes which discourages litigation is the requirement that an action must be instituted in the Supreme Court of the province. The high cost of suing in the Supreme Court, coupled with the embarrassment of having the invasion made public, has probably served to deter many potential litigants. In addition, in the absence of punitive damages, the sum recovered by a successful plaintiff is not likely to be large. In summary, as Professor Burns has noted[32]:

> ...these Acts do not grant real protection to the privacy interests they were set up to safeguard, at least at the most visible level. It may be alternatively conjectured that the existence of the Acts has resulted in a type of "preventive-legal" situation whereby people regulate their activities to take account of them. But at this stage of their evolution, the Acts have yet to reveal their efficacy.

Apart from these general reservations with respect to the utility of privacy protections in the provincial statutes, their applicability to the workplace appears extremely limited in light of the defences and exceptions provided by the Acts. Any employer who initiated a system of visual surveillance in any one of these three provinces would be able to argue that it was necessarily incidental to the defence of his property interests and that, consequently, there had been no actionable invasion of privacy.

---

32. P. Burns, "The Law and Privacy: The Canadian Experience", in The Canadian Bar Review, Vol. LIV, No. 1, (1976) p. 38.

THE UNITED STATES

A number of the American states have enacted privacy statutes similar to those in the western provinces. However, these are not as significant in the United States as is the vigorous development of the common law. American courts have not been as reluctant as their Canadian and British counterparts to give effect to claims for emotional distress caused by invasion of privacy. In addition, The American constitution provides under the 4th Amendment's protection against "unreasonable searches and seizures". However, this is only a protection for the citizen against state interference in his privacy, not a protection against interference by private persons. It therefore has no application to civil remedies between private parties, and particularly, it has no application in the workplace.

Common Law

Rather than being based in the Constitution, the American common law doctrine of protection of privacy arose out of the famous article written by Warren and Brandeis in 1890 entitled "The Right to Privacy".[33]

However, the scope of the doctrine is limited and, in many areas, it does not advance far beyond the Anglo-Canadian common law. For example, in the particular area of surveillance, which enjoys no protection in Britain or Canada, the American case law merely protects persons from surveillance which elicits private or confidential information. This limitation was made clear in Nader v. General Motors Corporation[34] where the defendant corporation carried out a concerted campaign of intimidation against the plaintiff who was a severe critic of the defendant. The intimidation included wiretapping of Nader's telephone and visual surveillance of him in public. The court stated:

> It should be emphasized that the mere gathering of information about a particular individual does not give rise to a cause of action under this theory. Privacy is invaded only if the information sought is of a confidential nature and the defendant's conduct was unreasonably intrusive. Just as a common law copyright is lost when material is published, so, too, there can be no invasion of privacy where the information sought is open to public view or has been voluntarily revealed to

---

33. Harvard Law Review, vol. 4, (1890) p. 193.

34. (1970), 307 N.Y.S. 3d. 647 (N.Y.C.A.)

> others... In order to sustain a cause of action for invasion of privacy, therefore, the plaintiff must show that the appellant's conduct was truly "intrusive" and that it was designed to elicit information which would not be available through normal inquiry or observation.

It can be seen that this limited protection against forms of surveillance which reveal private or confidential information would be of no avail in the workplace where a worker's actions are ordinarily visible to others.

It can be concluded that, although an American common law doctrine of invasion of privacy has developed, it has little or no application to surveillance in the workplace.

Legislation

It should be noted that the U.S. Omnibus Crime Control and Safe Streets Act, 1968, like the Canadian Criminal Code, prohibits electronic surveillance of oral communications except in certain limited exceptions where authorization is obtained by the police. Thus, in the United States, as in Canada, employees are protected against electronic interception of their private oral communications by their employers.

A number of American states have enacted statutes in an analogous area, that of the use of lie-detectors in the workplace. These states prohibit absolutely any requirement by an employer that a polygraph test be taken as a condition of employment. Similar legislation is currently proposed in Manitoba.[35]

To this extent, then, there is some legislative protection of privacy in the workplace in the United States, but it does not cover visual surveillance.

OTHER JURISDICTIONS

A large number of jurisdictions outside the compass of Anglo-American law have acted, to varying degrees, to protect the right to privacy. While a comprehensive international survey has not been undertaken, those European countries that have taken constitutional and/or legislative measures to restrict or prohibit the invasion of privacy include Austria, Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Sweden and Switzerland.[36] The fundamental differences between our legal system and those which prevail in continental Europe make them inappropriate models for provincial emulation.

---

35. 1979, Bill 20, s.10.

36. See, generally, Report of the Committee on Privacy op. c.t. Appendix J., pp. 308-326, Appendix P, pp. 338-339. See, also, Proceedings of the Eight International Symposium on Comparative Law, (Ottawa, 1971), pp. 87-210.

Chapter Four
ALTERNATIVE LEGAL AND OTHER RESPONSES

This chapter is designed to facilitate discussion of responses to the problems raised by electronic surveillance. Two types of non-legislative responses are offered as well as a range of legislative models of varying scopes. A few major advantages and disadvantages are noted to assist in evaluating the options but no attempt has been made to present an exhaustive list of "pros" and "cons".

The selection of an appropriate response, however, should take into consideration the extent to which electronic surveillance is a problem today or will be in the future, other potential infringements on personal privacy and human dignity (some of which are discussed in the paper within the context of the workplace), and whether the response should focus exclusively on the workplace. With respect to electronic surveillance a number of the alternatives which follow would require guidelines or exceptions so as to permit uses of monitoring equipment that are necessary or justified. Depending on the balance of interests between employee and employer, such exceptions could include employee health and safety, security and protection of the employer's property, training of employees, and monitoring of automated processes. Some would argue that, under certain circumstances, supervision of employees' productivity should be added to the list.

1
Rely on Common Law

At present, the common law permits an employer to conduct surveillance on his own property. This response accords stronger protection to an employer's property rights than to an employees interests in privacy and human dignity. However, the common law does not consist of fixed or rigid rules of jurisprudence, and it has shown a capacity to adapt to changing social values and conditions. It may be that the courts will recognize a cause of action for invasion of privacy or affront to dignity at some future time.

The major advantage to this response is flexibility - that is, remedies may be tailored according to the individual circumstances of a situation. The major disadvantage is that, since common law evolves slowly, the approach provides no immediate remedy. In the interim, employee interest would not be protected and disputes over electronic surveillance may disrupt industrial relations.

2 Voluntary Standards

The Government could, with the co-operation of employers and labour, develop guidelines or standards. This could be done through a tripartite commission or committee on either privacy in the workplace generally or specifically on electronic surveillance. Acceptance of the guide- lines by employers might be based upon recognition of the importance of privacy and human dignity in the workplace and of avoiding the negative effects of surveillance upon industrial relations.

The major advantage of this response is that it is voluntary. The major disadvantage is that success would depend on the co-operation of employers and employees. However, problems may persist in precisely those establishments - unionized and non-unionized alike - where the industrial relations climate is in disrepair.

3 Legislation

There are several courses of legislative action.

3a The Criminal Code

As previously noted, the Criminal Code makes it an offence to wilfully intercept private communications, except in certain limited situations hence prohibiting audio surveillance. An amendment to the Criminal Code coud be recommended to the Federal Government to prohibit electronic surveillance of persons generally, subject to exceptions for situations where such surveillance is deemed necessary for the protection of property or health and safety.

The major advantage of this response is that the right of privacy is not conditioned by location: it is consistent both inside and outside the workplace. The major disadvantage is that this response involves potentially lengthy and expensive procedures of criminal prosecution in the courts. It should also be noted that the Criminal Code is beyond Provincial jurisdiction.

3b A Privacy Act on The Western Provincial Model

The Legislature could pass a Privacy Act similar to the Acts currently in force in Manitoba, Saskatchewan, and British Columbia, but with clearer applicability to the workplace. A tort, or civil wrong, would be created and court action could be taken without proof of damages.

The major advantages to this response are that protection would be general in society rather than specific to the workplace and that all types of privacy issues could be covered rather than only surveillance. The major disadvantage, as derived from the experiences of the Western Provinces, is that costs and difficulties of bringing court action may make the protection ineffective. This disadvantage would be reduced if jurisdiction were given to the Small Claims Court or, in the alternative, to the County or Supreme Court.

3c A Privacy Ombudsman or Commission

A Privacy Act could be passed creating a privacy Ombudsman or Commission rather than providing for judicial decision. The Ombudsman or Commission could be given powers to investigate and provide remedies. In regard to the workplace this could be regarded as a specialized and institutionalized arbitration mechanism not limited to unionized establishments. The major advantage of this response would be the potential for inexpensive, accessible, and quick decisions. The major disadvantage might be delays in resolving issues caused by a potentially heavy workload.

3d Amend Civil Legislation

Rather than resorting to the Criminal Code or enacting a new statute on privacy, existing civil legislation could be amended to address the specific problem which has given rise to this issue - electronic surveillance in the workplace. The three Acts, specified below, which might be most appropriate for such amendment, are administered by the Ministry of Labour. The major advantages of this response are that the amendments could be more specifically framed for the environment of the workplace and perhaps more quickly implemented through an existing administrative structure. The major disadvantage is that the protection of privacy in the workplace may not have an equivalent beyond the workplace.

The amendments could provide for operation either through a pre-approval and licencing arrangement or through action only on a complaint basis. The former would have the advantage of not placing an onus on the employee to complain but the disadvantage of creating a larger and perhaps unnecessary demand for service and thus for a resulting administrative structure. The latter complaint approach would have the advantage of generating less demand and thus a smaller administrative structure but the disadvantage of placing the onus on an employee to complain.

i
The Employment Standards Act

The Employment Standards Act; could be amended to cover electronic surveillance in the workplace. The Act is directed at unionized and non-unionized establishments alike, but under this statute there is no provision for affirmative orders to rectify specific violations, other than orders relating to the payment of wages. Provision is needed for a cease and desist order or some such mechanism. This power to issue such orders could be vested in a referee appointed under Act, and investigations could be undertaken by a field staff located at several district offices throughout the Province.

ii
The Labour Relations Act

The Labour Relations Act; could be amended to cover electronic surveillance in the workplace, providing that the amendment extended the scope of the Act to to apply to non-unionized establishments as well as to unionized ones. The power to issue orders would be vested in the Ontario Labour Relations Board, which essentially is a judicial tribunal. The Board is located in Toronto, and hears cases in other locations as necessary.

iii
The Human Rights Code

The Human Rights Code; could be amended to cover electronic surveillance, but there is no existing right to privacy in the Code. If such a right were to be created, then its application might logically extend beyond the workplace. The power to investigate could be vested in the Commission, carried out by its field staff located at several district offices throughout the Province. The Commission could conciliate disputes and where conciliation fails could refer the matter to a board of inquiry for a binding decision.

SELECTED

BIBLIOGRAPHY

Hugh L. Black, Jr., "Surveillance and The Labour Arbitration Process" in Arbitration and The Expanding Role of Neutrals, Washington: Bureau of National Affairs, 1970.

Lee M. Burkey, "Employee Surveillance: Are There Civil Rights For The Man On The Job?" in New York University Conference On Labour Proceedings, Washington: Bureau of National Affairs, 1968.

Peter Burns, "The Law and Privacy: The Canadian Experience" in The Canadian Bar Review, Vol. LIV, No. 1, (March 1976).

Charles B. Carver, "The Inquisitorial Process in Private Employment" in Cornell Law Review, Vol. 63, No. 1, (Nov. 1977).

Dan Dorfman, "The End of Trust?" in Esquire, Vol. 41, No. 8, (April 24, 1979).

Martin N. Flics, "Employee Privacy Rights: A Proposal" in Fordham Law Review, Vol. 47, No. 2, (Nov. 1978).

J. R. Hackman and J. L. Suttle, Improving Life at Work: Behavioral Science Approaches to Organizational Change, Santa Monica: Goodyear, 1977.

D. Kramarsky, "Surveillance Systems: Management's Electronic Sentries" in Administrative Management, Vol. 27, (March 1976).

Privacy Committee (New South Wales), The Privacy Aspects of Employment Practices, Sydney: The Privacy Committee, 1977.

Privacy Committee (United Kingdom), The Rt. Hon. Kenneth Younger, Chairman, Report of The Committee on Privacy, London: Her Majesty's Stationery Office, 1972.

Privacy Protection Study Commission (United States), David F. Linowes, Chairman, Personal Privacy In An Information Society, Washington: U.S.G.P.O., 1977.

D. J. Purich, "The Truth About Lie Detectors" in Canadian Lawyer, Vol. 3, No. 2, (June 1979).

G. Robertson, "Absenteeism and Labour Turnover in Selected Ontario Industries," in Relations Industrielles, Vol. 34, No. 1, (1979).

Edward F. Ryan, "Protection of Privacy in Ontario: A Preliminary Study" in The Report on Protection of Privacy in Ontario, Ontario Law Reform Commission, H. Allan Leal (Chairman), Department of The Attorney General, 1968.

R. Tannenbaum and W. H. Schmidt, "How to Choose a Leadership Pattern," in Harvard Business Review, Vol. 36, (March-April 1958).

Alan F. Westin, Privacy and Freedom, Atheneum, New York, 1968.